REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Applicant advises that the attorney-docket number for the present application has changed as noted above and kindly asks that the Office update its records accordingly.

Claim Amendments

Claim 12 is amended clarifying the nature of each component in the masked signature and the regular signature. Claim 12 is also amended specifying that the sender had generated the masked signature in a secure computer system and referring to the signor as a verifier. Previous steps b) and c) of claim 12 have been amended and are now represented by new steps b), c) and d). Former step d) is now step e) and has been amended in accordance with the above amendments. Applicant notes that claim 12 now specifies the recovery of a point on an elliptic curve, the conversion of an element of the point to an integer, and the use of the integer to calculate the value r'. Support for these amendments can be found on page 7, lines 1-13.

Claims 13-16, 18-19 and 21 have been amended in accordance with the amendments to claim 12.

No new subject matter is believed to have been added by way of these amendments.

Regarding Information Disclosure Statement (IDS)

Applicant respectfully requests clarification regarding the Examiner's statement that an IDS was allegedly filed in the present application on 02/02/06. To Applicant's knowledge, no such IDS was filed. Moreover, the PAIR site for the USPTO also does not show such an IDS being filed on that date.

Claim Rejections – 35 U.S.C. 101

Claims 12-13 have been rejected under 35 U.S.C. 101 for allegedly being directed to non-statutory subject matter. Applicant respectfully traverses the rejections as follows.

Firstly, as noted above, claim 12 has been amended to indicate that the sender generates the masked signature components in a secure computer system.

To be statutory, a claimed computer-related process must either: (A) result in a physical transformation outside the computer for which a practical application in the technological arts is either disclosed in the specification or would have been known to a skilled artisan or (B) be limited to a practical application within the technological arts (section 2106 (IV)(B)(2)(b), MPEP).

Applicant submits that amended claim 12 is clearly restricted to a practical application within a cryptographic system and in secure computer systems, and as such, for at least that reason, claim 12 is believed to satisfy at least requirement (B) and the statutory requirement of 35 U.S.C. 101.

Applicant turns to *State Street Bank & Trust Co. v. Signature Financial Group*, 149 F.3d 1368 (Fed. Cir. Jul. 23, 1998) (hereinafter "*State Street*"). In *State Street*, the Court held that the transformation of data, representing discrete dollar amounts, by a machine through a series of mathematical calculations into a final share price, constitutes a practical application of a mathematical algorithm, formula, or calculation, because it produces "a useful, concrete and tangible result"-a final share price momentarily fixed for recording and reporting purposes and even accepted and relied upon by regulatory authorities and in subsequent trades.

In the present application, claim 12, e.g., is directed towards verifying a signature for a message sent in a data communication system, in part using components computed using a secure computer system. The method provides a secure verification for data communications, and has practical application in cryptography and cryptographic systems.

By performing the steps set out in independent claim 12, a useful concrete and tangible result is obtained, namely a verification of a tangible signature used in a tangible communication system for security purposes. Clearly, this is a concrete and tangible result. It is useful as recited in the claims in cryptographic systems where such verifications are paramount. It is well known that cryptographic operations involve the practical application of mathematics to generate, e.g., signatures for verification purposes. To perform these functions it is often necessary to utilize mathematics, e.g. to convert elements of a finite field to an integer or calculate signature components.

It is respectfully submitted that the claims of the present application, as in *State Street*, produce "a useful, concrete and tangible result". Namely, the claims of the present application involve the practical application of cryptographic operations to produce tangible results, namely the verification of a signature using a masked signature obtained by a verifier.

Accordingly, Applicant believes that all pending claims, namely claims 12-21 constitute statutory subject matter. Therefore, claims 12-21 are believed to comply with 35 U.S.C. 101.

Claim Rejections – 35 U.S.C. 112

Claim 12 has been rejected under 35 U.S.C. 112, second paragraph for allegedly being incomplete and omitting essential steps. Applicant advises that claim 12 includes a definition of an elliptic curve over a finite field used to recover a point therefrom. Accordingly, Applicant believes that claim 12 complies with 35 U.S.C. 112.

Claim 12 has also been rejected under 35 U.S.C. 112, second paragraph for being indefinite regarding the "first signature component". Applicant advises that amended claim 12 clearly defines each signature component and thus claim 12 is believed to comply with 35 U.S.C. 112.

Claim Rejections – 35 U.S.C. 103

Claims 12-21 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Applied Cryptography by Schneier ("Schneier") in view of the article "New Public-Key Schemes Based on Elliptic Curves over the Ring Zn" by Koyama ("Koyama"). Applicant respectfully traverses the rejections as follows.

Claim 12 is directed to a method for verifying a signature for a message *m* and requires that masked signature components (r, s, c) have been generated by a sender. As noted above, claim 12 is amended to more clearly define the nature of these components. The first component r is computed using a first short term public key derived from a first short term private key. The second component s is computed using a second short term private key on the message *m*, a long term private key and the first signature component r. The third component c is computed using the first and second short term private keys. This set of components (r, s, c) is used by the

verifier for verifying the signature. This is clearly recited in the preamble of amended claim 12.

In claim 12, the verifier first obtains a regular signature ($\bar{s}$, r) derived from the signature (r,s,c), where $\bar{s}$ is computed using the second signature component s and third signature component c, the nature of s and c being described above. The verifier then recovers a point on an elliptic curve defined over a finite field using the message and the component $\bar{s}$. The verifier then converts an element of the point to an integer and calculates a value r' from the integer, and then verifies that r' = r.

Applicant believes that amended claim 12 more clearly defines the nature of the signature components and respectfully maintains that Schneier fails to teach what is recited in claim 12. Moreover, the additional teachings taken from Koyama fail to provide what is missing from Schneier and in fact provides no direction or motivation for applying the teachings to Schneier, and thus are entirely inapplicable.

The Examiner relies on a passage in pages 509-510 of Schneier. This passage outlines the Guillou-Quisquater Signature Scheme, where Alice computes signature components d and D as $d = H(M,T)$ and $D = rB^d \bmod n$ respectively. The component T is computed using a random integer r, and the function H is a hash function. Alice sends the components d and D along with the message M and her credentials j to Bob. Bob uses d and D to compute a representation of the component T, namely T' and then calculates a representation of d, namely d' using the message M and the representation T'. Bob then verifies the signature by comparing d with d'.

Firstly, the Examiner has equated the components d and D with the components (r, $\bar{s}$), and further states that "said component being derived from a first (random integer r) and second signature components (B) generated by a signor...". Applicant believes that amended claim 12 more clearly defines the regular signature and how it is derived from the masked signature. For instance, $\bar{s}$ in claim 12 is derived from components s and c, which are derived as outlined above (and clearly recited in the preamble of claim 12). However, neither component d nor component D in Schneier are derived in such a way. For example, component d is derived from a message M and component T.

Although the component s is derived in part from the message *m*, there is no teaching in Schneier that would lead a person skilled in the art to believe that the component T is equivalent to the second short term private key and short and long term public keys. Schneier is entirely silent in that regard. Therefore, $\bar{s}$ and d are completely different and thus, Applicant submits,

cannot be considered equivalent.

Similarly, the component D is derived from the integer r and the component d. Clearly this is not equivalent to how $\bar{s}$ is derived. In claim 12, component c is derived from the first and second short term private keys. A careful review of Schneier will reveal that there is no mention of deriving a signature component in such a way. Equating D in Schneier to either $\bar{s}$ or r is believed to be improper and cannot be considered equivalent components.

Schneier also does not teach obtaining a pair of signature components from a set of three components as recited in claim 12. Schneier simply does not teach utilizing masked signature components such as (r, s, c) recited in claim 12. In fact, Schneier only teaches Bob obtaining d and D directly from Alice and does not include a step of obtaining one component from two other components generated by Alice. Schneier is entirely silent in that regard. Moreover, claim 12 requires that the regular signature having components $(r, \bar{s})$ be derived from (r, s, c). Schneier does not have an equivalent step. Applicant believes that even taking a "bit from here" and a "bit from there", the combination of Schneier and Koyama still fails to teach what is recited in claim 12.

Secondly, each step in claim 12 relies in part from what is previously recited in the claim. For example, verifying r'=r requires calculating r' from one of the coordinate pairs, which are recovered using $(r, \bar{s})$ etc. Applicants believe that they have shown above that Schneier does not teach deriving $(r, \bar{s})$ as recited in claim 12. Accordingly, Schneier fails to teach any of the steps recited in claim 12 for at least that reason.

Finally, according to MPEP 2143, in order to establish a *prima facie* case of obviousness, the references, when combined, must teach every element recited in the claim and there must be found, some motivation in the teachings to either combine the teachings or modify at least one of the teachings to arrive at what is claimed. Applicant believes that not only is there no motivation to combine the references, Koyama does not even teach what is missing from Schneier and thus a *prima facie* case of obviousness has not been established.

Therefore, Applicant believes that claim 12 clearly distinguishes over the prior art cited by the Examiner, and as such is in condition for allowance. Claims 13-21 being ultimately dependent on claim 12 are also believed to distinguish over the prior art.

Summary

In view of the foregoing, Applicant believes that all pending claims, namely claims 12-21 are patentably distinguished over the references cited by the Examiner and are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,

Ralph A. Dowell
Attorney for Applicant
Registration No. 26,868

Date: August 16, 2006